

Serial No.: 09/718,583
Attorney Docket No.: 10005173-1

REMARKS

The Office Action dated November 9, 2005 contained a final rejection of claims 1-16. The Applicants have amended claims 1, 10, and 15. Claims 1-16 are in the case. Please consider the present amendment with the attached Request for Continued Examination (RCE) under 37 C.F.R. § 1.114. This amendment is in accordance with 37 C.F.R. § 1.114. Reexamination and reconsideration of the application, as amended, are requested.

The Final Office Action rejected claim 10 under 35 U.S.C. § 112, first paragraph.

The Applicants respectfully traverse this rejection and submit that the claims comply with 35 U.S.C. § 112, first paragraph. However, in an effort to expedite the prosecution of this case, the Applicants have amended claim 10 to remove "without creating a domain agent between the first server and the plural servers."

The Office Action rejected claims 1-3 and 9-11 under 35 U.S.C. § 102(e) as being anticipated by Sampson et al. (U.S. 6,339,432 B1). Also, the Office Action rejected claims 4-8 and 12-16 under 35 U.S.C. § 103(a) as being unpatentable over Sampson in view of Goldberg et al. (U.S. Patent No. 5,823,879 A).

The Applicants respectfully traverse these rejections based on the amendments to the claims and the arguments below.

The Applicants respectfully submit that the rejections under 35 USC 102 are overcome in light of the amendments to the claims. Namely, the Applicants' claimed invention now includes accessing the services of the second server from the user and based on the received identifier if both identifiers are authenticated, authenticating the user and the first server based on the first and second identifiers and allowing access to the second server by linking the user to the second server through the first server. This is advantageous because it is done without requiring the use of a cookie, in other words, a cookie request from the client is not necessary if both identifiers are authenticated, which eliminates the use of cookies when connecting to the second server.

In contrast, Sampson does not disclose, teach, or suggest all of the claimed features. First, although the Examiner alleged that Sampson provides authentication without the use of cookies via a multi-domain token, the Applicants respectfully disagree

Serial No.: 09/718,583
Attorney Docket No.: 10005173-1

with this interpretation of Sampson. This is because even if the multi-domain tokens are used by Sampson to authenticate, as argued by the Examiner on pages 11-12 of the Final Office Action, the overall system, including the multi-domain token mechanism in Sampson is specifically designed to ultimately cause the required cookies to be stored on the user's computer, as admitted by the Examiner on page 11, section 8.

As such, unlike the Applicants' claimed invention, the central 'Multi-Domain Token Server' in Sampson requires the ability to communicate with the primary server and each of the secondary servers via an additional 'Domain Agent' component. For example, Sampson states that "[S]uch a mechanism is provided by the following components of access control system 220: Primary Domain Agent 242, Secondary Domain Agents 262 and 282, and Multi-Domain Token Server 208. These elements may be servers that cooperate with each other to provide a multi-domain access control system... (see col. 5, lines 17-21 and FIG. 2 of Sampson).

As explicitly disclosed in Sampson on col. 5, lines 46-59 that the "...Primary Domain Agent 242 transmits the Multi-Domain Token to the browser, and causes the browser to connect to the Secondary Domain Agent. When the browser connects to the Secondary Domain Agent, the browser transmits a Multi-Domain Token to the Secondary Domain Agent. The Secondary Domain Agent then transmits to Multi-Domain Token Server 208 a request to verify that the Multi-Domain Token represents a user that has been authenticated by access control system 220. Upon receiving from Multi-Domain Token Server 208 a message confirming that the user has been authenticated, the Secondary Domain Agent transmits to the browser access control cookies that are associated with the domain of the Secondary Domain Agent." *[emphasis added]*.

Consequently, the argument provided by the Examiner that the multi-domain token mechanism in Sampson is used for authenticating is inconsequential because the Examiner admits on page 11, section 8 of the Office Action that cookies are ultimately employed and required to be stored on the user's computer, unlike the Applicants' claimed invention.

Next, the Examiner alleged that "by employing negative limitations, any reference, teaching, authentication without using the terminology "cookies" so long as

Serial No.: 09/718,583
Attorney Docket No.: 10005173-1

the functionality of the claimed invention is taught clearly teaches the claimed invention. The applicant(s) are suggested to amend the claim language to explicitly recite the functional features that which teach away from the prior art than relying on negative limitations."

However, the Applicants respectfully disagree with the Examiner's above statement because, clearly, according to the case law and the MPEP, negative limitations are not prohibited. If the Applicants' claimed negative limitations are distinguishable and provide advantages not appreciated by the references they cannot be ignored, which is what the Examiner attempted to do in this case. In Re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). MPEP 2143.

Specifically, the Background of the Invention of the Applicants disclosure provides that "...some web servers store on a client data terminal (the consumer's PC) small data files, (also referred to as "objects") known as "cookies." When a user of a client data terminal first links to a web site, the host server obtains registration information from the consumer and stores the registration information and/or an assigned personal identifier in a cookie that is stored on the client data terminal...The use of cookies by host servers has become so widespread that issues of consumer privacy and the storage of cookies on consumers' computers are topics of heated public debate. Some consumers even attempt to block the storage of cookies on their computers or disable cookies already stored there. Furthermore, cookies do not address the needs of the mobile user who often has access to computers spread over distances...Therefore, a need exists for a method and apparatus whereby a consumer can link to a second web site through a first web site and access the services of the second web site without being required to provide registration information or a personal identifier and without the use of a "cookie." [*emphasis added*].

Therefore, since the claimed features are proper and all of them are not disclosed by Sampson, it cannot anticipate the claims, and hence, the Applicants submit that the rejection should be withdrawn.

With regard to the rejections under 35 U.S.C. 103, even though the combined references do not disclose, teach or suggest all of the Applicant's features, Sampson cannot be combined with Goldberg et al. because Sampson teaches away from the

Serial No.: 09/718,583
Attorney Docket No.: 10005173-1

Applicants' claimed invention. In particular, as argued above, Sampson is specifically designed to ultimately cause the required cookies to be stored on the user's computer, as admitted by the Examiner on page 11, section 8. Thus, since Sampson requires cookies in order to allow access, Sampson will not work without having cookies installed and functioning on the user's machine, notwithstanding the Examiners' argument that "...the multi-domain tokens are employed to authenticate."

Therefore, since Sampson actually does in fact require the use of cookies, and the Applicants' claimed invention eliminates cookies, the intended function of Sampson would be destroyed if the use of cookies were eliminated, like in the Applicants' claimed invention, which is a clear teaching away. Moreover, Sampson would be rendered inoperable if authentication was performed without the use of cookies and user access would always be denied. As a result, when taking the entire disclosure of Sampson into consideration, it is clear that from col. 5, lines 46-59 that Sampson requires "access control cookies", unlike the Applicants' claimed invention. Hence, this "teaching away" prevents obviousness from being established by combining these references. This failure of the cited references, either alone or in combination, to disclose, suggest or provide motivation for the Applicant's claimed invention indicates a lack of a prima facie case of obviousness. W.L. Gore & Assocs. V. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983). (MPEP 2143).

Accordingly, the combined cited references cannot render the Applicant's invention obvious. This failure of the cited references to disclose, suggest or provide motivation for the Applicant's claimed invention indicates a lack of a prima facie case of obviousness (MPEP 2143).

With regard to the rejection of the dependent claims, because they depend from the above-argued respective independent claims, and they contain additional limitations that are patentably distinguishable over the cited references, these claims are also considered to be patentable (MPEP § 2143.03).

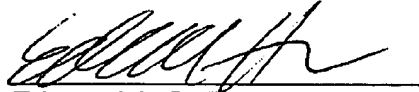
In view of the arguments and amendments set forth above, the Applicants respectfully submit that the rejected claims are in immediate condition for allowance. The Examiner is therefore respectfully requested to withdraw the outstanding claim rejections and to pass this application to issue. Additionally, in an effort to expedite and

Serial No.: 09/718,583
Attorney Docket No.: 10005173-1

further the prosecution of the subject application, the Applicants kindly invite the Examiner to telephone the Applicants' attorney at (818) 885-1575. Please note that all correspondence should continue to be directed to:

Hewlett Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

Respectfully submitted,
Dated: February 9, 2006



Edmond A. DeFrank
Reg. No. 37,814
Attorney for Applicant